AMENDMENTS TO THE SPECIFICATION

Please amend paragraphs [0019] and [0020] as follows:

> FIG. 6a illustrates an example of the logical operations for determining a risk of identity theft fraud, in accordance with an embodiment of the present invention.
>
> FIG. 6b [[7]] is a block diagram showing logical operations for appending certain information to addresses in performing analysis for determining a risk of identity theft fraud, in accordance with an embodiment of the present invention.

Please amend paragraph [0045] as follows:

> With respect to FIG. 6b [[7]], a brief description of the logical operations performed in determining the data appended from demographic data (block 30). In selecting demographic data to append to an address, first an attempt is made to match the name and address (block 27). If there is a match, then the demographic data is the appended from that file. However, if there is not a match for both name and address, then there is an attempt made to match the address. If a match is made, then the demographic data for the address is appended. Also, for the area defined by a Zip+4 or Zip code+4, a demographic data for that area is appended. For instance, if information related to length of residence was being appended to each address, then first, a search would be made to match the name and address to the file containing such information. If a match is made, the length of residence data from that file would be appended. If such a match is not made, then an attempt would be made to match the address only. If there is a match, then the length of residence for the last person at the address would be appended. Also, the length of residence for the residences in the Zip+4 would be appended (or an average of the length of residences for the residences in the Zip+4 would be appended).

Please amend paragraphs [0223] and [0224] as follows:

> As shown in FIG. 2, once information has been appended to the addresses, then a score is created based on all the data (block 82). Generally, statistical models are used to derive a score, which is used to predict the risk of fraud. At block 82, a score is created based on the data associated with the request and the appended data. FIG. 6a shows the logical operations for determining a score in accordance with one embodiment of the present embodiment. As shown is FIG. 6a, as shown in block 180, the first step is to analyze the demographic data appended to each of the addresses and derive information used to predict the risk of fraud. Next, as shown in block 182, a score is calculated based on the weights placed for each of the selected variables. In one embodiment of the present invention the following variables have been selected to be used in the model to predict the risk of fraud: (1) a variable that is based on the change in the financial make-up of the two addresses; (2) a variable that identifies records that were confirmed through third party data to match the name at a given address; (3) a variable that is based on the

home value between the two addresses; (4) a variable that is based on the distance of the move for the change of address; (5) a variable that is based on whether the type of housing (e.g., apartment, non-apartment, single family home) has changed for the current address in comparison with the reference address or old address; (6) a variable that is based on whether the application address or the new address is a building (i.e., not an apartment or a home, rather something other than an apartment or a home); (7) a variable based on whether the new application address, the new address or current address is a warm address; (8) a variable that is based on the difference in internet usages for the Zipcode+4 area for the two addresses; and (9) a variable that is based on the average length of stay at the residence at the Zip+4 area code for the reference address or the old address (when there is an address change requested). Then, the second step is to use the model to obtain a score to predict the risk of fraud. Each of these variables will be discussed in turn.

The first variable is based on the change in the financial make-up of the two addresses. In one embodiment of this model, this variable is called "Valuel." This variable analyzes the change in the financial make-up of the reference address, the old address (e.g., in address change or account takeover situations), or FROM address (e.g., old address) and new application address, the new address, or the TO address (e.g., the address to which it has been changed). It is a composite of three demographic variables: Income, Net Worth and Home Ownership. In one embodiment, to derive the composite information the following steps are used. First, the difference in income is determined. As described with respect to FIG. 6b [7]], to determine the difference in income, for both addresses (e.g., new application address and reference address in risk of fraud relating to a new application or as will be described later, reference or old and new addresses in a takeover situation), income for the respective address is appended by matching name and address to the appropriate demographic file. If there is not a match by both name and address, then a search is made to match at by address only to find income. If there is not a match by address only, then the Zip+4 for an address is used and the average income for that Zip+4 is appended to the address. If there is still not a match, then the mean income for all individuals is assigned. For instance, the mean income for all individuals may be assigned, when a Zip+4 for a particular address cannot be determined or when demographic data cannot be located for the address of a Zip+4 area.

Please amend paragraph [0294] as follows:

Another way to look at the performance of the model is to look at a Power of Segmentation summary chart, shown in FIG. 7. This is sometimes also referred to as a ROC curve or Lorenz Diagram. This view shows how many cumulative fraud records are identified for each level of screening.

Please amend paragraphs [0306] and [0307] as follows:

> FIGS. 8-15 show alternatives to the basic method described with respect to FIG. 2 for use in account takeover situations. That is, the basic logical operations of appending information to the addresses and calculating a score as described with references to FIGS. 2-6b [[7]] would be used. As described with respect to FIG. 2, in determining fraud with respect to a new application the reference address is usually linked to the applicant's identity, not necessarily the address on the new application form. As described above, usually, in a new application situation, the reference address is obtained from a credit bureau. However, in the takeover situation, the old address or the FROM address would be the reference address and the address to which it is changed to is the new address (e.g., the TO address). A customer may want each change of address analyzed to determine a risk of fraud and match to subsequent media requests, a customer may want the change of address analyzed only when such a request is matched to a media request, or a client may want each change of address analyzed for risk of fraud. Each of these situations will be discussed in turn with reference to FIGS. [[7]] 6b-13.
>
> FIGS. 9, 11, and 12 show the logical operations for an embodiment in which an analysis is performed for each address change and a match is made for subsequent media requests. As shown in FIG. 9, 11, and 12, the logical operations for analyzing the risk of fraud is the same as that described and shown in FIGS. 2-6b [[7]]. That is, information is appended to the old address (the address before the change of address request)--which for takeover situation would be considered a reference address--and to the new address (i.e., the address it was changed to). Then, a score would be derived using the model described with reference to FIG. 6a. However, as shown in block 300, there is an address change file that maintains the change in address for a particular account. Also, as shown in block 302, a media request file is maintained. A media request may include a request for financial instruments such as checks or credit cards. In addition, as shown in block 304, a scored history file is maintained to store the score based on the analysis done (consistent with the analysis as described in FIG. 2) for an account in which there was a change in address. When a media request is made, it is checked against the scored history file. If there is a match in terms of an address change in the same account on which the media request is made, business rules--which may be supplied by the customer--are used to determine whether to honor the media request. Some factors that may be used include the time lapse between the media request and the address change and the risk of identity theft fraud as determined by the scoring.

Please amend paragraph [0309] as follows:

> FIGS. 13-15 show the process described with respect to FIGS. 2-6b [[7]] being applied in the case when each address change is scored, but no additional steps are performed with respect to media requests.

Please add the following paragraph after paragraph [0020]:

> FIG. 7 illustrates a Power of Segmentation summary chart.